Lightweight Ciphers for Internet of things: A Survey

Amarpreet Singh, Sandeep Singh, Gurpreet Singh

Abstract*: Resource Constrained devices such as embedded system, Internet of Things based network and its applications areas are becoming a part of human's life. These networks comprises of intelligent nodes interacting with each other in a significant way offering plenty of services. These networks are still having various vulnerabilities and which in turn requires a lot of security measures. Basically, Internet of Things (IoT) system suffers from various attacks and hence some appropriate solution is required for the protection. There are some security challenges that need to be addressed which could be followed for the design of Secure IoT system. The paper presents a comprehensive survey of 33 symmetric lightweight ciphers with original implementations on 0.09µm, 0.13µm, 0.18µm, 0.25µm and 0.35µm technologies used in constrained environments with the different metrics.

***Index Terms*: WSN, RFID, Gate Equivalency, Constrained Devices**

I. INTRODUCTION

Resource constrained devices are characterized by computing power, gate equivalency (Area) and memory requirements [1]. Among those, IoT devices are tremendously increasing year by year and it is expected that by 2020 the figure will reach in billions. Therefore, all these devices require the security parameters which are basically provided by the means of cryptographic principles. In general, to make an algorithm cryptographically secure, the following security requirements must be fulfilled:

Confidentiality(C): The protection of data from unauthorized disclosure.

Integrity(I): The assurance that the data received are exactly as sent by an authorized entity.

Availability(A): Ensuring timely and reliable access to and use of information. Among the symmetric and asymmetric cryptographic algorithms, the symmetric algorithms fulfill the security goals of Confidentiality/Integrity/Availability (CIA triad) [2] efficiently and are computationally less challenging [3]. Also, the Symmetric ciphers have two variants as block ciphers and stream ciphers. The performance of a given algorithm is measured and analyzed both in software and hardware contexts i.e. low power, energy consumption, complexity (time/space) and gate equivalency/Area (GE) factors. In Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Array (FPGA) implementations the area [1] is expressed in µm2 and resource utilization. Typically, one Gate Equivalency (GE) is equivalent to one NAND gate. The traditional cryptography algorithms such as Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA-256) and Rivest Shamir Adleman/Elliptic Curve Cryptography (RSA/ECC) proved well on systems which have good processing and memory capabilities, but they don't fit to Wireless Sensor Networks (WSN) and Radio Frequency Identification (RFID) networks. In RFID and WSN network devices, security is highly constrained by the number of gates available as well as power draining requirements. So, AES or any other traditional algorithm is not suitable. Therefore, to guarantee security in IoT the lightweight cryptography algorithms/methods are the suitable solutions for memory limited and processing constrained devices. A number of methods are proposed for lightweight cryptography by National Institute of Standards (NIST) and ISO/IEC which can be used in IoT and RFID devices. The Section II describes a complete survey of various lightweight ciphers according to key size, block size, structure, and area (GEs). Section III presents the discussions and Section IV concludes the paper.

II. DIFFERENT LIGHTWEIGHT CIPHERS

A general cipher has three parts encryption, decryption and key expansion modules which offers good security. Researchers find the cipher implementation a critical task as there is vast research articles have been published which addressed various aspects such as throughput, energy, latency and gate equivalency. We tried to focus latest ciphers for low resource devices which in turns covers both software and hardware implementations. These implementations on symmetric aspect have five basic structures: Substitution-Permutation (SPNs), Feistel Networks,

Revised Manuscript Received on May 06, 2019

Amarpreet Singh, Research Scholar, Department of Computer Science ,Chandigarh University, Mohali, Punjab, India.
Dr. Sandeep Singh, Department of Computer Science, Chandigarh University Mohali, Punjab, India.
Dr. Gurpreet Singh Department of Computer Science, Punjab Institute of Technology, Rajpura, India.

Add-Rotate XOR (ARX), LFSR and hybrid [3].

M CRYPTON: Chae Hoon *et al.* proposed a 64 bit block cipher mCrypton [4] with three 64 bits , 96 bits and 128 bits key size based on the original implementation of Crypton with efficient and precise implementation both in hardware and software aspects. The original prototype requires 12 number of rounds, 3500 to 4100 GEs for both encryption/decryption and about 2400 to 3000 GEs for encryption only (with an average of 2949) on 0.13µm technology and have SP network. The cipher with 12 full rounds stands resistive against the differential and linear cryptanalysis, since the complexity of these analyses depends upon number of active S-boxes and their characteristics. The number of nonzero nibbles is also a measure to ensure the defense against these analyses.

HIGHT: Deukjo Hong *et al.* described a low resource hardware implementation uses a new block cipher HIGHT [5] with 64-bit block length and 128-bit key length. The algorithm was good enough as a security encryption algorithm requires 3048 GEs on 0.25µm technology. It uses 32 round Iterative structure which is variant to generalized Feistel structure. The cipher defends well against differential and linear cryptanalysis, since differential attack on 13-round HIGHT recovers the subkeys of 12^{th} and 13^{th} rounds with 262 plaintexts and linear attack on 13-round. HIGHT recovers the 36 bits of the sub-keys of 1^{st}, 12^{th} and 13^{th} rounds with 257 plaintexts. PRESENT: Bogdanov *et al.* proposed an ultra lightweight block cipher called PRESENT [6] proves its applicability on both security and hardware aspects. It uses 64 bits block length with 80 bits and 128 bits key lengths having SP structure consists of 31 rounds. The PRESENT-80 requires 1569.93(≈1570) GEs when implemented on 0.18µm technology. Linear cryptanalysis of PRESENT is well defended by linear approximation to four rounds. As, the design of PRESENT is bitwise this gives good strength against integral and bottleneck attacks. LBLOCK: Wenling *et al.* introduced a new block cipher called LBLOCK [7] of 64 bits block and uses 80 bits key size with hardware implementation of 1320 GEs on 0.18µm technology. It counters the known attacks such as differential cryptanalysis, linear cryptanalysis and related key attacks. It employs a variant Feistel structure with 32 rounds. KLIEN: Zheng *et al.* introduced a new family of lightweight ciphers called KLEIN [8] designed for resource constrained devices which uses SP Structure with 12/16/20 as number of rounds for KLEIN 64/80/96 key length with a block size of 64 bits. KLEIN 64/80/96 measures 2475/2629/2769 GEs on data paths of 64 bits. The structure is also resistive to linear and differential attacks, key schedule attacks, Integral attacks, Algebraic attacks and Side Channel Attacks.DES/DESL/DESX/DESXL: Gregor *et al.* proposed variants to original DES, DESL, DESX, DESXL [9] which works on 64 bits block size using a key 56/56/184/184 bits having Feistel structure with 16 rounds and 2309/1848/2629/2168 GEs is implemented. Also, it is shown that DESL is highly resistive to Linear and Differential cryptanalysis and Davies Murphy Attack.

$PRINT_{CIPHER}$: Lars *et al.* presented two block ciphers $PRINT_{CIPHER-48}$ and $PRINT_{CIPHER-96}$ [10] works on 48/96 bits block size using 80/160 bits key size having SP structure with 48/96 rounds and 402/503/726/967 GEs respectively. The designs utilize the properties of IC printing technology and also $PRINT_{CIPHER-48}$ is analyzed with respect to Differential/Linear cryptanalysis, Algebraic attacks, Related Key Attacks, Statistical Saturation Attacks.

KATAN/KTANTAN: Christophe *et al.* proposed two block ciphers [11] based on stream ciphers with 32/48/64 bits block size using 80 bits key having LFSR structure requires 254 rounds. KATAN family requires 802/927/1054 GEs where as KTANTAN requires 462/588/688 GEs. Both KATAN and KTANTAN family is secure enough to differential attacks, combined attacks, related key differential attacks, algebraic attacks and is more secure to cube attacks than TRIVIUM.

TWINE: Tomoyasu *et al.* presented a 64 bit lightweight block cipher called TWINE [12] with 80/128 bit key length using Feistel structure requires 36 rounds. TWINE uses generalized Feistel Structure with 16 branches. TWINE-80 with Round base/Serialized architecture requires 1503/1116 GEs whereas TWINE-128 with Round base architecture requires 1866 GEs. TWINE-80 is vulnerable to Impossible differential attacks (against the 23rd round)/Saturation attack as it is using Feistel/Generalized structure. TWINE is resistant to Slide attacks but it is observed that a variant to Meet in the Middle called BICLIQUE Attack may work.

PUFFIN: Huiju *et al.* introduced a new compact block cipher called PUFFIN [13] based on an Involutional SP structure with 64 bit block size using 128 bit key size requires 32 rounds. PUFFIN cipher requires 2577 GEs and also, the cipher is resistant to differential cryptanalysis and whereas in linear cryptanalysis it is almost impractical as it requires 264 known plaintexts against compact cipher. Non regularity in the key schedule algorithm makes new cipher highly immune against related key attacks and due to use of 4 bits selected inversion and permutations in the key space, the cipher is resistant to Weak Keys attack. LED: Jian *et al.* proposed a lightweight block cipher LED [14], [15] works on 64 bits block with a 64/80/96/128 bits key length having SP structure requires 32/48/48/48 rounds. LED cipher operates with two sets Hardwired key and flexible key arrangements requires 688/690/695/700 and 966/1040/1116/1265 GEs. MITM attacks on 8 out of 32 and 16 out of 48 rounds are exploited for LED-64 and LED-128.

The Design of LED is very similar to Even Mansour Scheme which have been used with differential analysis and the same is used 12 to 16 rounds (out of 32) for LED-64 and 16 to 24 rounds (out of 48) for LED-128.

RECTANGLE: Wentao *et al.* proposed a bit slice technique [16] based ultra-light weight block cipher which allows fast implementations for multiple platforms works on 64 bits block size with 80 bits or 128 bits key size having SP structure requires 25 rounds. RECTANGLE-80 with round based/serialized architecture requires 1467/1066 GEs. Whereas RECTANGLE-128 operates with 1787 GEs. The 25 rounds of RECTANGLE is strong enough and highly resistive against Differential Cryptanalysis (Multiple).

EPCBC: Huihui *et al.* proposed a cipher designed for Electronic Product Code Encryption [17] works on 48/96 bits block size with 96 bits key size having SP structure requires 32 rounds. EPCBC cipher requires 1008/1333 GEs. EPCBC cipher defends well against differential as well as linear cryptanalysis (seven 4-round blocks in 28 rounds). Integral attack on EPCBC 48/96 and EPCBC 96/96 uses some differentials (same as in PRESENT) and also balance property of the structure gets violated which does not allow the increase in number of rounds, therefore EPCBC is well protected to Integral attacks. Also, Related key differential, Statistical Saturation, Higher order, Slide, Algebraic attacks doesn't appear any threat to EPCBC.

MIBS: Maryam *et al.* proposed a new lightweight called MIBS [18] uses block length of 64 bits with 64 bits or 80 bits key lengths of having Feistel Structure requires 32 rounds. MIBS requires 1396 GEs on 0.18µm technology. The cipher is secure against differential and linear cryptanalysis and even, a variant called Differential-linear which uses differential characteristics to linear approximations is not applicable to full rounds. Bi-linear cryptanalysis another variant doesn't seem to be practical attack against MIBS. Another line of attacks such as Algebraic, Slide and Related Key are unable to affect the MIBS.

HUMMINGBIRD: Daniel *et al.* described a combination of block and stream ciphers [19] with 16 bit block size uses 256 bit key size and 80 internal states require 20 rounds. The original Hummingbird uses 1023 GEs Four identical 16 bit block ciphers with SP structure with 16 bit block size and 64 bit key is used consists of 4 regular rounds and one final round that includes key mixing and S-box Substitution. HUMMINGBIRD is highly resistive to common attacks such as Birthday Attack, Differential and Linear Cryptanalysis. Also, due to complexity in internal state transition in encryption scheme, even structural attacks can't be applied to cipher. Another line of attacks such as cube, algebraic, slide, related key, Interpolation/high order differential and complementation property even doesn't seem to be threat to the respective cipher. Its variant HUMMINGBIRD-2 uses 128 bit secret keys and 64-bit Intialization Vector(IV) produces a MAC for each message.

SIMON & SPECK: Beaulieu *et al.* proposed a family of block ciphers SIMON & SPECK [20] in replacement to original AES. Both ciphers uses various $N_b/N_k/N_r$(SIMON)/N_r(SPECK) parameters 32/64/32/22, 48/72/36/22, 48/96/36/23, 64/96/42/26, 64/128/44/27, 96/96/52/28, 96/144/54/29, 128/128/68/32, 128/192/69/33 & 128/256/72/34 bits as respective block size, key size and no. of Rounds requires Feistel structure. The GEs for size 48/96, 64/96, 64/128, 96/96 and 128/128 ranges from 763-1396 for ASIC implementation. The SIMON and SPECK block ciphers consists of 10 different block ciphers with a variant block and key size, since there is no threat identified on any variant to SIMON or SPECK family member.

SEA: Standaert *et al.* introduced a scalable encryption algorithm called SEA [21] for resource constrained small devices operates on various block, key and word sizes uses Feistel structure with variable number of rounds. The $SEA_{n,b}$ requires 'n' bits for plaintext/key size, 'b' for processor or word size, n_b as number of words per Feistel branch with n_r as number of rounds. SEA with n-bit loop architecture using various n, b & n_r parameters requires 3758 to 5764 GEs whereas with b-bit architecture requires 4472 to 6046 GEs. SEA is resistive against square attacks as the number of rounds (n_b + b/2⌋) and the use of addition mod 2^b are enough to provide defense. Even, to defend against the Truncated and Impossible differentials the number of rounds must be 2.(n_b + b/2⌋).Also, SEA well defends against the Interpolation, Slide , Related Key, Algebraic attacks and it is recommended that the total number of rounds to stand completely resistive against known attacks must be (3n/4) + 2.(n_b + b/2⌋). CLEFIA: Taizo *et al.* proposed a 128-bit block cipher CLEFIA [22] which uses 128/192/256 bits key size fully compatible with AES requires 18/22/26 as number of rounds based on 4-branch generalized Feistel structure. This proposal on the basis of round architecture requires 5979/4950 GEs for 128 bit key length and 8536/8482 GEs for 192/256 bits key length on 0.09 µm technology whereas with serial based architecture it requires 2996 GEs on 0.13 µm technology for 128 bit key length. The full round CLEFIA is highly resistive to differential and linear cryptanalysis. Another line of attacks such as Impossible differential cryptanalysis, saturation and related key attacks doesn't seem to be threat to full round CLEFIA. Moreover, some attacker manage to get Impossible differential attack against 13 and 14 rounds with 2146 and 2212 encryptions as time complexities. Later on a new kind of attack called

Improbable differential cryptanalysis has been identified which crypt-analyzed the 13/14/15/ rounds of CLEFIA for the 128/192/256 bits key size with more time complexity.

PICCOLO: Kyoji *et al.* introduced 64-bit block cipher PICCOLO [23] supports 80 and 128 bits key size using mixture of 4 branches general Feistel structure followed by a byte RP permutation. PICCOLO 64/80 and 64/128 requires 25/31 rounds with having round- based and serialized architecture implementation. Both variants 64/80 & 64/128 with serialized architecture requires 683/758 GEs and with round architecture need 1136/1197 GEs. The full round of PICCOLO with both the configurations defends against differential and linear attacks. Another line of attack Boomerang type attack is difficult to accomplish as two sub ciphers for PICCOLO have F-Functions (7-atleast). Related key differential attacks and three subset meet in the middle attack (MITM) even unable to violate the PICCOLO as it has whitening keys which makes stronger enough against these attacks.

TWIS: Ojha *et al.* described 128-bit block TWIS [24] works with 128 bit key having key scheduling and data processing parts. TWIS uses 2-branch generalized Feistel network which uses whitening structure at the beginning\ and at the end of the structure. The cipher works with 10 rounds using S-box and diffusion matrix that provides diffusion properties. TWIS assures the avalanche effect by having effect on round keys on changing single bit of key, effect on cipher text on changing 1-bit of key keeping plaintext constant and effect on cipher text on changing 1-bit of plaintext keeping key constant and even TWIS is tested best to statistical testing results in bits produced which are random in nature.

ITUBEE: Ferhat *et al.* proposed a software based lightweight cipher [25] specifically for 8-bit based platform devices. The cipher operates on 80-bit block with a 80-bit key having Feistel structure requires 20 number of rounds. The existing cipher with 20number of rounds doesn't allow differential and linear attacks as it is difficult to count the number of S-boxes with differential and linear hull effects. Even, meet in the middle attack doesn't seem threat to MITM as after 3 successive rounds the output gets changed with each key bit. Biclique attack as an extension to MITM even is unable to reduce the security measures more than 1-bit. Another line of attacks such as related key differential, impossible differential and self similarity attacks doesn't affect the security level of ITUBEE.

NOEKEON: Daemen *et al.* introduced a block cipher [26] with 128-bits block size operates with 128 bits key size having SP network requires 16 rounds. The cipher requires 2862 GEs on 0.18µm, 2880 GEs on 0.13µm and 2604 GEs on 0.35µm technologies. The cipher is resistive to differential and linear cryptanalysis as there doesn't exists a 4-round differential trails with a predicted prop ratio above 2^{-48} and linear trails with a correlation coefficient above 2^{-34}. Due to bit oriented nature of cipher, it doesn't have truncated differentials and stands resistive to even interpolation attack which is based on manipulation of algebraic expressions.

ICEBERG: Standaert *et al.* introduced a fast involutional block cipher [27] uses 64 bits block size and 128 bits key size requires 16 number of rounds. The cipher uses SP network and requires 5817 GEs on 0.18µm technology for reconfigurable hardware implementations. Variants of differential and linear attacks such as boomerang, rectangle, multiple linear and non linear approximations of outer rounds are unable to touch the security boundaries of ICEBERG. Also, the expressions of S-boxes are not simple, so it defends best against the interpolation attacks. Slide, related key, high order differential and square attacks doesn't appear to be serious line of attack on ICEBERG.

MIDORI: Banik *et al.* proposed energy efficient ciphers [28] of 64 bits and 128 bits with key size 128 bits requires 16/20 number of rounds have a SP network variant structure. The MIDORI-64 requires 1542/1638 GEs whereas MIDORI-128 requires 2522/2714 GEs on STM 90/65nm or 0.09µm technology with round-based architecture. Both Midori 64/128 doesn't have any differential and linear cryptanalysis even when get reduced to 7 and 13 rounds. To counter boomerang attack even after 8 rounds and 14 rounds, it has at least 32 and 64 active S-boxes. Both the variants have 3-round full diffusion property, therefore full rounds are enough to provide the security boundaries. Midori-64 and Midori-128 defends against the Meet in the middle attack as the white keys are present in the begin/end and due to actual constraint of key orders PRINCE: Borghoff *et al.* proposed a latency optimized block cipher [29] which uses 64 bits block cipher with 128 bits key divided in to two parts 64 bits each (k0||k1) which is further mapped to 192 bits. The first k0 is called whitening keys whereas k1 for 12-round block cipher is referred as PRINCECORE. Each round of PRINCECORE uses a key addition, an S-box layer, a linear layer and the addition of a round constant. The PRINCE-64 requires 2286 GEs on STM 90nm or 0.09 µm technology. PRINCE has atleast 16 active S-boxes with 4 consecutive rounds which is sufficient enough to provide resistance against differential and linear attacks. Even it is imagined that the cipher doesn't show any strong differential or hull effects. Also, PRINCECORE found good only up to 4 rounds against the Meet in the Middle attack. In order to defend against the algebraic attack, the proposed equation system contains 43264 and 5376 quadratic Boolean terms that doesn't allow the linearization to take place. TwoFish: Schneier *et al.* proposed a 128 bit block cipher [30] which uses a variable length key upto 256 bits. The cipher requires 16-round Feistel Network with a bijective function (F).

Two Fish requires 14000 gates and is efficiently performed over 32-bit CPUs, 8-bit smart cards and dedicated VLSI hardware. It is also imagined that brute force attack is the only attack that happened more effectively than any other attack. To attack this cipher, any linear cryptanalysis for the given keyspace would require atleast $2^{120.8}$ chosen plaintexts and Twofish stands resistive to multiple linear, non-linear, generalized linear, partitioning and differential cryptanalysis. Due to large algebraic degree, the Twofish is well resistive to Interpolation attack.

LEA: Deukjo *et al.* introduced 128-bit block cipher [31] with 128/192/256 bit key size. The cipher requires 24/28/32 number of rounds with all three variations in key size. The cipher requires 3826 GEs implemented on 0.13µm technology and has ARX structure. The cipher is tested against each common attack and firstly, the maximum number of rounds has been identified for available characteristics, thereafter best N-round characteristics have been used. To counter differential attacks, some of the characteristics have been applied to 11 rounds from Round 0 to Round 10 and attack 12 rounds for 128 bit key. The possibility of 13-round attack for 192 bit keys and 14-round attack for 256 bit keys is considered, since no weaknesses have been identified. Also, the possibilities of n-round attack for 128/192/256 bits key is considered for zero correlation, boomerang, impossible differential, integral, and differential-linear attacks.

CHAM: Boonwook *et al.* introduced a family of block ciphers [32] with 64/128,128/128, 128/256 as respective block-size/key-size .The cipher has generalized 4-branch Feistel structure based on ARX operations uses 80/80/96 number of rounds for all three variants. The CHAM 64/128 requires 665/859/727 GEs for bit serial architecture and 826/1110/985 GEs for round based architecture implemented on IBM130, UMC180 and UMC90 technology. The CHAM 128/128 requires 1057/1296/1084 GEs for bit serial architecture and 1499/1899/1691 GEs for round based architecture implemented on IBM130, UMC180 and UMC90 technology. Whereas, CHAM 128/256 requires 1180/1481/1256 GEs for bit serial architecture and 1622/2087/1864 GEs for round based architecture on IBM130, UMC180 and UMC90 technology. Various essential number of rounds have been estimated in order to ensure the security against differential and linear, boomerang, impossible differential, zero correlation linear cryptanalysis attacks.

QTL: Lang *et al* proposed a new ultra lightweight cipher [33] of 64 bits with 64/128 bits key variants. The cipher requires 16/20 number of iterative rounds for both key variants and uses fast diffusion of the substitution permutation structure as a variant to generalized Feistel network structure. Both the cipher key variants requires 1026/1207 GEs implemented 0.18µm technology. Since, for three rounds the MDP and MLP is 2-42. Therefore, it is expected that the 16/20 rounds of QTL-64 and QTL-128 has a good resistance differential and linear cryptanalysis. Also, QTL-64 has 10752 quadratic equations with 4096 variables, whereas QTL-128 has 13440 quadratic equations with 5120 variables which doesn't give any solution to find the master key, so cipher doesn't allow algebraic attack to take place.

TEA: Wheeler *et al.* introduced simplified block cipher [34] with 64 bits block size using 128 bits key size having Feistel Structure. A total of 64 rounds is recommended and TEA requires 2355GEs implemented 0.18µm technology.

SKIPJACK : SKIPJACK [35] block cipher was designed by NSA and declassified in 1998 with a 64 bits block size using 80 bit key length having Unbalanced Feistel Structure. The algorithm has two rounds named Rule A and Rule B with each round using linear feedback shift register with an additional keyed G permutation. The Skipjack has been exposed to impossible differential attack which breaks 31 rounds out of 32 rounds. Also, a truncated differential attack is noticed which targets 28 rounds of Skipjack.

III. DISCUSSIONS

Various generations of original ciphers using different parameters are examined in Table I. A complete summary of different ciphers is carried out by considering Gate Equivalency (GE) as key factor in terms of hardware implementations on 0.09µm, 0.13µm, 0.18µm, 0.25µm and 0.35µm technologies.

We have examined and compared these symmetric ciphers on 0.09µm, 0.13µm, 0.18µm, 0.25µm and 0.35µm implementations. The Figure 1-4 illustrates the best hardware implementation of above technologies in terms of GE.

On 0.09µm technology CHAM has lesser GE among its counterparts TWINE, MIDORI, PRINCE and CLEFIA. Moreover, KTANTAN family on 0.13µm has least GE whereas the LEA has higher 3826GE compared with

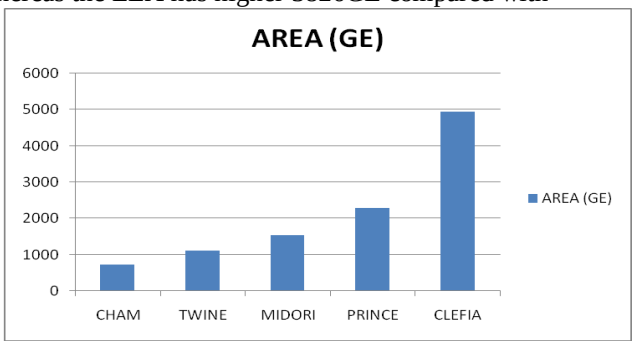

Fig 1: Best Hardware Implementation on 0.09 µm

PICCOLO, SIMON, KATAN, SPECK and other ciphers.

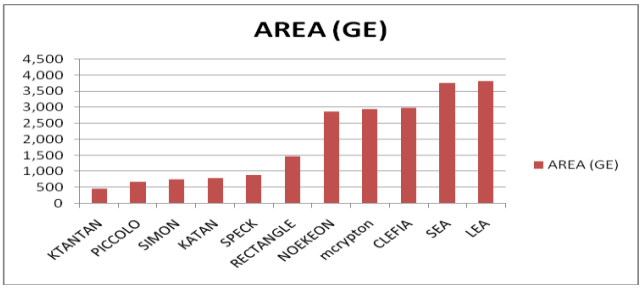

Fig 2: Best Hardware Implementation on 0.13 µm

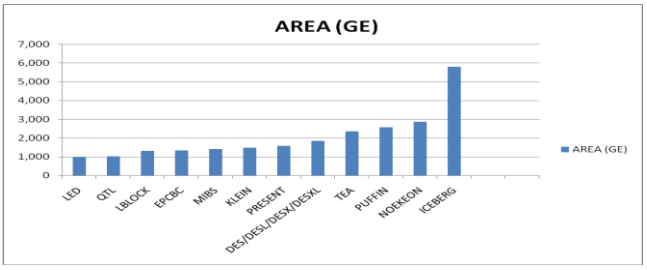

Fig 3: Best Hardware Implementation on 0.18 µm

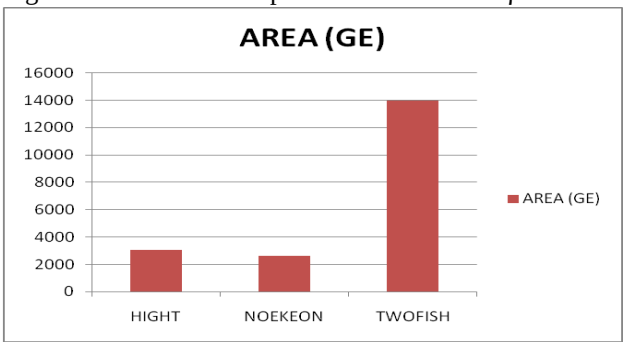

Fig 4: Best Implementation on 0.25µm & 0.35µm

With 0.18µm technology (Fig. 3), PRINTCIPHER with 80 bit key has lesser GE compared with MIBS, LBLOCK and ICEBERG exceeds the 5000 GE(5817) boundary.

On 0.25µm (Fig. 4) only HIGHT with 3048 GE and on 0.35µm NOEKEON with 2604 GE, Two Fish with 14000 GE takes the edge

IV. CONCLUSION

This paper covered an exclusive survey of latest symmetric lightweight ciphers such QTL, CHAM, RECTANGLE and MIDORI along with other having their basic requirements and original parameters in the field of lightweight symmetric cryptography. Moreover, a comparison of these ciphers in terms of gate equivalency on different technologies is conducted. Symmetric lightweight cryptography being the best solution in resource constrained environment can help the researchers in finding abundant opportunity in exploring other ciphers with having possibilities of attack on them. Also, one can further extend the research in exploring the public key light weight ciphers in the area of lightweight cryptography suitable for embedded systems/resource constrained devices.

Table I Lightweight Ciphers with basic parameters (original)

Cipher Name	Year	Block Size(n) (in Bits)	Key Size(k) (in Bits)	Structure	No. of Rounds	AREA (GE)	Technology	Resistance to attacks
Cham	2018	64/128	128/256	4-branch Feistel based on ARX	80/96	(n, k) 668(64,128),826(64,128) 859(64,128),1110(64,128) 727(64,128), 985(64,128) 1057(128,128),1499(128,128) 1296(128,128),1899(128,128) 1084(128,128),1691(128,128) 1180(128,256),1622(128,256) 1481(128,256),2087(128,256) 1256(128,256),1864(128,256)	(Bit Serial, Round Based) IBM-130 UMC-180 UMC-90 IBM-130 UMC-180 UMC-90 IBM-130 UMC-180 UMC-90	LC,DC, Boomerang, Impossible Differential, Zero Correlation linear cryptanalysis
Qtl	2016	64	64/128	SP	16/20 Iterative	1026 (64 bit Key) 1207 (128 bit key)	0.18 µm	LC,DC & Algebraic
Rectan Gle	2015	64	80/128	SP	25	1467 (80-bit key), 1787 (128-bit key)	0.13 µm	Multiple DC
Midori	2015	64/128	128	SP	16/20	1542 (64-bit Block) 2522 (128-bit Block)	STM 90nm	LC, DC, Boomerang,& MITM

Lea	2014	128	128/192 /256	ARX	24/28/ 32	3826	0.13 µm	Differential, Boomerang, Integral, Zero Correlation
Simon	2013	32/48/64/ 96/128	64/72/ 96/128/ 144/192/ 256	Feistel	32/36/ 42/44/ 52/54/ 68/69/ 72	1000 (64,128) 1317 (128,128) 763 (48,96) 838 (64,96) 984 (64,96)	0.13 µm	Traditional such as Related Key Attack
Speck	2013	32/48/64/ 96/128	64/72/ 96/128/ 144/192/25 6	Feistel	22/23/ 26/27/ 28/29/ 32/33/ 34	1127 (64,128) 1396 (128,128) 884 (48,96) 984(64,96) 1134 (64,96)	0.13 µm	Traditional such as Related Key Attack
Klein	2012	64	64/80/96	SP	12,16, 20	1528 (96-bit key) 1478 (80-bit key)	0.18 µm	Linear, Differential, Key Schedule, Integral, Algebraic,
Prince	2012	64	128	SP	12	2286	STM 90nm	Meet in the Middle, Algebraic
Epcbc	2011	48/96	96	SP	32	1333	0.18 µm	LC,DC, Integral, Related key differential, Statistical Saturation, Higher Order, Slide, Algebraic
Lblock	2011	64	80	Feistel	32	1320	0.18 µm	LC,DC, Related Key
Led	2011	64	64/80/ 96/128	SP	32/48/ 48/48	966 (64-bit Key) 1040 (80-bit Key) 1116 (96-bit Key) 1265 (128- bit Key)	0.18 µm	Meet in the Middle (MITM)
Piccolo	2011	64	80/128	Feistel	25/31	683 (80-bit Key) 1136 (80-bit Key) 758 (128-bit Key) 1197 (128-bit Key)	0.13 µm	Differential, Linear, Boomerang, Related Key Differential, MITM
Twine	2011	64	80/128	Feistel	36	1116/1503/1866	0.09 µm	Saturation, Slide
Print	2010	48/96	80/160	SP	48/96	(n, k) 402 (48,80) 726 (96,160)	0.18 µm	LC, DC, Algebraic, Related key , Statistical Saturation
Katan	2009	32/48/64	80	LFSR	254	802 927 1054	0.13 µm	Differential, Combined, Related Key, Algebraic, Cube
Ktantan	2009	32/48/64	80	LFSR	254	462 588 688	0.13 µm	Differential, Combined, Related Key, Algebraic, Cube attacks
Mibs	2009	64	64/80	Feistel	32	1400	0.18 µm	LC,DC, Bilinear, Algebraic, Slide,Related key
Puffin	2008	64	128	SP (Involutional)	32	2577	0.18 µm	LC,DC, Related key & Weak keys

Clefia	2007	128	128/192/256	Gen. Feistel	18/22/26	4950 5979 2996	0.09 µm 0.09 µm 0.13 µm	LC & DC, Impossible differentials, Saturation & Related key
Present	2007	64	80/128	SP	31	1570	0.18 µm	LC, Structural, Algebraic, Key Schedule
Des/Desl/Desx/ Desxl	2006	64	56/184	Feistel	16	2309 1848 2629 2168	0.18 µm	LC,DC & Davies Murphy
Hight	2006	64	128	Gen. Feistel	32 (Iterative)	3048	0.25 µm	LC&DC
Mcryp Ton	2006	64	64/128/ 192	SP	13	2949(avg.)	0.13 µm	LC&DC, algebraic, related key
Sea	2006	48/96 /144 (Variable)	48/96 /144 (Variable)	Feistel	Variable	3758	0.13 µm	Square, Truncated & Impossible differentials, Interpolation,
Iceberg	2004	64	128	SP	16	5817	0.18 µm	Boomerang, Rectangle, Interpolation
Noekeon	2000	128	128	SP	16	2862 2880 2604	0.18 µm 0.13 µm 0.35 µm	LC,DC , Interpolation & Truncated differential
Twofish	1998	128	upto 256 bits (Variable)	Feistel	16	14000	0.35 micron CMOS/0.35 µm	All LC and DC, Interpolation
Tea	1994	128	64	Feistel	64(recomm.)	2355	0.18µm	Equivalent Key

REFERENCES

1. Mohd BJ, Hayajneh T, Vasilakos AV. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications. 2015 Dec 1;58:73-93.
2. William Stallings, Lawrie Brown "Computer Security, Principles and Practice". 2010 edition
3. Hatzivasilis G, Fysarakis K, Papaefstathiou I, Manifavas C. A review of lightweight block ciphers. Journal of Cryptographic Engineering. 2018:1-44.
4. Lim CH, Korkishko T. mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors. International Workshop on Information Security Applications 2005 Aug 22 (pp. 243-258). Springer, Berlin, Heidelberg.
5. Hong D, Sung J, Hong S, Lim J, Lee S, Koo BS, Lee C, Chang D, Lee J, Jeong K, Kim H. HIGHT: A new block cipher suitable for low-resource device. International Workshop on Cryptographic Hardware and Embedded Systems 2006 Oct 10 (pp. 46-59). Springer, Berlin, Heidelberg..
6. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher. International Workshop on Cryptographic Hardware and Embedded Systems 2007 Sep 10 (pp. 450-466). Springer, Berlin, Heidelberg.
7. Wu W, Zhang L. LBlock: a lightweight block cipher. International Conference on Applied Cryptography and Network Security 2011 Jun 7 (pp. 327-344). Springer, Berlin, Heidelberg.
8. Gong Z, Nikova S, Law YW. KLEIN: a new family of lightweight block ciphers. International Workshop on Radio Frequency Identification: Security and Privacy Issues 2011 Jun 26 (pp. 1-18). Springer, Berlin, Heidelberg.
9. Leander G, Paar C, Poschmann A, Schramm K. New lightweight DES variants. International Workshop on Fast Software Encryption 2007 Mar 26 (pp. 196-210). Springer, Berlin, Heidelberg.
10. Knudsen L, Leander G, Poschmann A, Robshaw MJ. PRINTcipher: a block cipher for IC-printing. International Workshop on Cryptographic Hardware and Embedded Systems 2010 Aug 17 (pp. 16-32). Springer, Berlin, Heidelberg.
11. De Canniere C, Dunkelman O, Knežević M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. Cryptographic Hardware and Embedded Systems-CHES 2009 2009 (pp. 272-288). Springer, Berlin, Heidelberg.
12. Suzaki T, Minematsu K, Morioka S, Kobayashi E. Twine: A lightweight, versatile block cipher. ECRYPT Workshop on Lightweight Cryptography 2011 Nov 28 (Vol. 2011).
13. Cheng H, Heys HM, Wang C. Puffin: A novel compact block cipher targeted to embedded digital systems. Digital System Design Architectures, Methods and Tools, 2008. DSD'08. 11th EUROMICRO Conference on 2008 Sep 3 (pp. 383-390). IEEE.
14. Benadjila R, Guo J, Lomné V, Peyrin T. Implementing lightweight block ciphers on x86 architectures. International Conference on Selected Areas in Cryptography 2013 Aug 14 (pp. 324-351). Springer, Berlin, Heidelberg.
15. J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw, The LED Block Cipher, Cryptographic Hardware and Embedded Systems, CHES 2011, Springer, LNCS, 6917, 2011, pp.326-341.
16. Zhang W, Bao Z, Lin D, Rijmen V, Yang B, Verbauwhede I. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences. 2015 Dec 1;58(12):1-5.
17. Yap H, Khoo K, Poschmann A, Henricksen M. EPCBC-a block cipher suitable for electronic product code encryption. International Conference on Cryptology and Network Security 2011 Dec 10 (pp. 76-97). Springer, Berlin, Heidelberg.
18. Izadi M, Sadeghiyan B, Sadeghian SS, Khanooki HA. MIBS: a new lightweight block cipher. International Conference on Cryptology and Network Security 2009 Dec 12 (pp. 334-348). Springer, Berlin, Heidelberg.

19. Engels D, Fan X, Gong G, Hu H, Smith EM. Hummingbird: ultra-lightweight cryptography for resource-constrained devices. International Conference on Financial Cryptography and Data Security 2010 Jan 25 (pp. 3-18). Springer, Berlin, Heidelberg.
20. R. Beaulieu, S. Douglas, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, The SIMON and SPECK Families of Lightweight Block Ciphers, IACR Cryptology ePrint Archive, 2013, 404.
21. F. Mace, F.-X. Standaert, and J. Quisquater, ASIC implementations of the block cipher sea for constrained applications, RFID Security (RFIDsec 2007), Malaga, Spain, 2007,pp. 103114
22. Shirai T, Shibutani K, Akishita T, Moriai S, Iwata T. The 128-bit blockcipher CLEFIA. International Workshop on Fast Software Encryption 2007 Mar 26 (pp. 181-195). Springer, Berlin, Heidelberg.
23. Shibutani K, Isobe T, Hiwatari H, Mitsuda A, Akishita T, Shirai T. Piccolo: an ultra-lightweight blockcipher. International Workshop on Cryptographic Hardware and Embedded Systems 2011 Sep 28 (pp. 342-357). Springer, Berlin, Heidelberg.
24. Ojha SK, Kumar N, Jain K. TWIS–a lightweight block cipher. International Conference on Information Systems Security 2009 Dec 14 (pp. 280-291). Springer, Berlin, Heidelberg.
25. Karakoç F, Demirci H, Harmancı AE. ITUbee: a software oriented lightweight block cipher. International Workshop on Lightweight Cryptography for Security and Privacy 2013 May 6 (pp. 16-27). Springer, Berlin, Heidelberg.
26. J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen, On Noekeon, no!, 2001,http://gro.noekeon.org/
27. Standaert FX, Piret G, Rouvroy G, Quisquater JJ, Legat JD. ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware. International Workshop on Fast Software Encryption 2004 Feb 5 (pp. 279-298). Springer, Berlin, Heidelberg.
28. Banik S, Bogdanov A, Isobe T, Shibutani K, Hiwatari H, Akishita T, Regazzoni F. Midori: a block cipher for low energy. International Conference on the Theory and Application of Cryptology and Information Security 2014 Dec 7 (pp. 411-436). Springer, Berlin, Heidelberg.
29. Borghoff J, Canteaut A, Güneysu T, Kavun EB, Knezevic M, Knudsen LR, Leander G, Nikov V, Paar C, Rechberger C, Rombouts P. Prince–a low-latency block cipher for pervasive computing applications. International Conference on the Theory and Application of Cryptology and Information Security 2012 Dec 2 (pp. 208-225). Springer, Berlin, Heidelberg.
30. Schneier B, Kelsey J, Whiting D, Wagner D, Hall C, Ferguson N. Twofish: A 128-bit block cipher. NIST AES Proposal. 1998 Jun 15;15.
31. Hong D, Lee JK, Kim DC, Kwon D, Ryu KH, Lee DG. LEA: A 128-bit block cipher for fast encryption on common processors. International Workshop on Information Security Applications 2013 Aug 19 (pp. 3-27). Springer, Cham.
32. Koo B, Roh D, Kim H, Jung Y, Lee DG, Kwon D. CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices. International Conference on Information Security and Cryptology 2017 Nov 29 (pp. 3-25). Springer, Cham.
33. Li L, Liu B, Wang H. QTL: a new ultra-lightweight block cipher. Microprocessors and Microsystems. 2016 Aug 1;45-55.
34. D. Wheeler and R. Needham, TEA, a Tiny Encryption Algorithm, Fast Software Encryption (FSE 1994), Springer, LNCS, 1008, 1994, pp.363-366.
35. Knudsen L, Wagner D. On the structure of Skipjack. Discrete Applied Mathematics. 2001 Jul 15;111 (1-2):103-16.

AUTHORS PROFILE

Amarpreet Singh, received his B.Tech in Computer Science Engineering from SLIET, Longowal (PTU) in 2003 and M.Tech in Computer Science and Engineering from DAVIET, Jalandhar (PTU) in 2009. He has teaching experience of 15 years. He has published various research papers and his area of interest is wireless and mobile communications. He is currently pursuing Ph.D. degree in Computer Science and Engineering from Chandigarh University,Gharuan, Mohali(Punjab).

Dr. Sandeep Singh Kang is working as Professor in Department of Computer Science & Engineering at Chandigarh University.Gharuan, Mohali(Punjab). He did his B.tech, M.Tech and Ph.D in Computer Science & Engineering. He has published more than 70 research papers and one book. He has 15 Years Teaching experience in various colleges and universities. He is the life member of ISTE.

Dr. Gurpreet Singh is doctorate from the Department of Computer Science and Engineering, Thapar University, Patiala, Punjab (India) and is also working as Associate Professor in the Department of Computer Science and Engineering, Punjab Institute of Technology, Rajpura, Punjab (India). He has received his M.Tech. (CSE) and B.Tech. (CSE) from IKG Punjab Technical University, Jalandhar, Punjab (India). He has published over 70 papers in reputed journals and conferences in India and Abroad. He is also certified from CISCO (CNAP) in 2002 and Microsoft (MCSD, MCP) in 1998. He has more than 16 years of experience in teaching. His research topics are mainly focused in area of Swarm Intelligence, Ant Colony Optimisation, Mobile Adhoc Networks, Network Congestion Control Protocols and Routing Protocols (both in wired and wireless environment).

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication